UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/607,007	06/29/2000	Thomas P. Hardjono	2204/A46	7322

34845 7590 02/09/2005

STEUBING AND MCGUINESS & MANARAS LLP
125 NAGOG PARK
ACTON, MA 01720

EXAMINER	
CHOUDHURY, AZIZUL Q	
ART UNIT	PAPER NUMBER
2145	

DATE MAILED: 02/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/607,007	HARDJONO ET AL.	
	Examiner	Art Unit	
	Azizul Choudhury	2145	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 September 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-149* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-149* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 June 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6/29/00*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Detailed Action

This office action is in response to the correspondence received on September 10, 2004.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-149 are rejected under 35 U.S.C. 102(b) as being anticipated by Mittra (US Pat No: US005748736A).

1. With regards to claims 1, 16, 28, 40, 61, 68, 75, 78, 87, 99, 113, 122 and 145, Mittra teaches a communication system comprising:

- a plurality of multicast devices forming a shared multicast distribution tree;
- a host device;
- a key server; and
- a designated device, separate from the key server, through which the host device accesses the shared tree, wherein:
- the host device obtains access information from the key server for the host device to access the shared tree, the access information including authentication information unique to the host device;

- the designated device obtains the access information associated with the host device from the key server for enabling the host device to access the shared tree;
- the host device sends an access control message to the designated device to join the shared tree; and
- the designated device uses the access information to authenticate the host device before adding the host device to the shared tree.

(A communication system is able to be a method, apparatus, communication message and computer program. Mittra discloses a multicast network wherein; any member of the multicast network may be a sender or a receiver (column 4, lines 5-19). There exists a device in Mittra's design (the GSC) that maintains group membership information and hence authenticates hosts and receivers in the multicast network (column 7, line 64 – column 8, line 10). In addition, Mittra discloses that if desired, separate key distribution centers (KDC, equivalent to the claimed key server) are also usable (column 4, lines 53-54, Mittra). Furthermore, authentication for each host device must be unique as claimed. This is because to each host, the number of clients available and eligible is different. Hence, the authentication information for each must be different as claimed. Plus, Mittra's design allows the network to be a tree architecture (column 6, lines 1-19). Furthermore, the process of host authentication in networks (including multicast networks) is a standard set by the IGMP version 2 protocol. Furthermore, Mittra's disclosure expresses the methods by which devices may request and gain access to a multicast network by communicating (sending and

receiving of data by the devices) with an authentication host (the GSC). Finally, Mittra's disclosure teaches that certificates expire and new ones are created and sent with messages (column 11, lines 39-42, Mittra) (expiration of certificates is equivalent to the key expiration date of claim 145). It is inherent that since the certificate expiration is noticed and new certificates are sent, that the claimed access information comprising expiration date information is also present within Mittra's design).

2. With regards to claim 2, Mittra teaches a communication system wherein the key server includes logic for authenticating the host device and generating the access information for the host device to access the shared tree (Servers are simply devices that are able to fulfill requests made by client machines. Mittra's design contains GSCs which act as servers. It is with the GSC that members of the multicast network (including the hosts) authenticate themselves with keys (column 7, line 64 – column 8, line 10). Since authentication occurs, it is inherent that the logic to do so is present as well, as claimed).

3. With regards to claims 3, 20, 64 and 71, Mittra teaches a communication system wherein the key server provides the access information to the host device over a secure communication channel (A communication system is able to be a method, computer program and an apparatus. The network of Mittra's design uses secure channels (column 8, lines 3-10)).

4. With regards to claims 4, 23, 65 and 72, Mittra teaches a communication system wherein the key server provides the access information to the designated device using a unicast distribution mechanism (A communication system is able to be a method, computer program and an apparatus. Mittra's design allows for both unicast and multicast (column 6, lines 1-19)).

5. With regards to claims 5, 24, 66 and 73, Mittra teaches a communication system wherein the key server provides the access information to the designated device using a multicast distribution mechanism (A communication system is able to be a method, computer program and an apparatus. Mittra's design allows for both unicast and multicast (column 6, lines 1-19)).

6. With regards to claims 6, 25, 67 and 74, Mittra teaches a communication system wherein the key server provides the access information to the designated device using a broadcast distribution mechanism (A communication system is able to be a method, computer program and an apparatus. Mittra's design allows for multicast networks (column 6, lines 1-19), which is a broadcast network. Furthermore, Mittra discloses that any network may be used for the design (column 4, lines 60-61)).

7. With regards to claims 7 and 26, Mittra teaches a communication system wherein the designated device requests the access information from the key server upon receiving the access control message (A communication system is a method. A device

that requires authentication will need authentication with the key server (GSC) and hence the two must communicate with each other (column 8, lines 3-14)).

8. With regards to claim 8, Mittra teaches a communication system wherein the key server provides the access information to the plurality of multicast devices forming the shared tree (The GSC (key server) of Mittra's design maintains all the group membership information (column 7, line 64 – column 8, line 2)).

9. With regards to claims 9, 17, 29, 36, 37, 46, 62, 69, 76, 83, 84, 88, 96, 106, 129, 146, and 148, Mittra teaches a communication system wherein the access information comprises: a token identifier; and an authentication key (A communication system is able to be a method, computer program, communication message and an apparatus. Mittra's design performs authentication (column 8, lines 3-10). During authentication, the access information must contain an id of some form to distinguish it; hence a token identifier must be present. Mittra discloses the use of a member id that is equivalent to the claimed token identifier (column 7, lines 52-54). In addition, authentications keys are present in Mittra's design).

10. With regards to claims 10, 30, 47, 77, 89, 95, 107 and 130, Mittra teaches a communication system wherein the access control message comprises the token identifier (A communication system is able to be a method, computer program, communication message and an apparatus. Mittra's design performs authentication

(column 8, lines 3-10). During authentication, the access information must contain an id of some form to distinguish it; hence a token identifier must be present. Mittra discloses the use of a member id that is equivalent to the claimed token identifier (column 7, lines 52-54)).

11. With regards to claims 11, 38, 85 and 97, Mittra teaches a communication system wherein the access control message is an Internet Group Management Protocol (IGMP) join request including the token identifier (A communication system is able to be an apparatus, computer program and a method. Mittra's design performs authentication (column 8, lines 3-10). During authentication, the access information must contain an id of some form to distinguish it; hence a token identifier must be present. Mittra discloses the use of a member id that is equivalent to the claimed token identifier (column 7, lines 52-54). In addition, Mittra's design allows for the use of any network (column 4, lines 60-61) hence, any protocol that functions with the network chosen is acceptable).

12. With regards to claim 12, Mittra teaches a communication system wherein the designated device joins the shared tree on behalf of the host device upon authenticating the host device (All devices to enter the multicast in Mittra's design must be authenticated since all devices are able to be receivers and senders (column 8, lines 3-10)).

13. With regards to claim 13, Mittra teaches a communication system wherein the shared tree is a Protocol Independent Multicast (PIM) shared tree, and wherein the designated device sends a PIM join request upstream toward a rendezvous point device in order to join the shared tree on behalf of the host device upon authenticating the host device (Mittra's design allows for any network to be used and hence any protocol as well (column 4, lines 60-61)).

14. With regards to claims 14, 15 and 58, Mittra teaches a communication system wherein the designated device forwards the access control message to a neighboring device upon failing to authenticate the host device using the access information (A communication system is a method. Since each member of Mittra's multicast is both a receiver and a sender, each needs to be informed constantly what members are present. Otherwise, the multicast would be unable to distribute data properly).

15. With regards to claims 18, 48, 50, 108, 131 and 147, Mittra teaches a method wherein the access information further comprises an expiration date for the authentication key (A computer program, apparatus and communication message are able to be methods. Mittra's design uses authentication (column 8, lines 3-10). For an authentication key to function properly, it inherently must possess an expiration method of some form).

16. With regards to claim 19, Mittra teaches a method wherein the access information further comprises a public key (The access information is used during authentication. During authentication, keys (no limitation was made on what type of key) are used between the two authenticating parties (column 8, lines 3-10)).

17. With regards to claim 21, Mittra teaches a method wherein the communication message is a group key management communication message (The authentication process occurs between a device and the GSC in Mittra's design (column 8, lines 3-10). The GSC maintains group key management and hence the communication message is a group key management communication message).

18. With regards to claim 22, Mittra teaches a method wherein sending the access information to the designated device for the host device comprises: sending a communication message including the access information to the designated device over a secure communication channel (Mittra's design uses secure channels (column 8, line 3).

19. With regards to claims 27 and 109, Mittra teaches a method wherein the access token comprises: a group identifier for identifying a multicast group; a host identifier for identifying the host device; a token identifier for identifying the access token; an authentication key for the host device; an expiration date for the authentication key; a server identifier for identifying a key server; and a public key for the key server (An

apparatus is able to be a method. Mittra's design performs authentication (column 8, lines 3-10). During authentication, the access information must contain ids of some form to distinguish it; hence a token identifier along with ids for other parameters must be present. Mittra discloses the use of a member id that is equivalent to the claimed token identifier (column 7, lines 52-54). In addition, it is disclosed that keys are used and hence that must be within the access token as well to properly fulfill the authentication process (column 8, lines 3-10)).

20. With regards to claims 31 and 90, Mittra teaches a method further comprising: generating authentication information using the access information; and sending the authentication information to the designated device (A computer program is a method. Mittra's design performs authentication (column 8, lines 3-10). During authentication, the claimed steps must be performed).

21. With regards to claims 32, 53, 79, 91, 114 and 137, Mittra teaches a method wherein generating the authentication information using the access information comprises generating a digital signature using the access information and a predetermined digital signature scheme (An apparatus and computer program are able to be a method. Mittra's design has authentication means (column 8, lines 3-10). In authentication, it is very common to use digital signature schemes and hashes. Mittra as to what form of authentication to perform provides no limitation).

22. With regards to claims 33, 54, 80, 92, 115 and 138, Mittra teaches a method wherein the predetermined digital signature scheme comprises a keyed hash function (An apparatus and computer program are able to be a method. Mittra's design has authentication means (column 8, lines 3-10). In authentication, it is very common to use digital signature schemes and hashes. Mittra as to what form of authentication to perform provides no limitation).

23. With regards to claims 34, 55, 81, 93, 116 and 139, Mittra teaches a method wherein the keyed hash function comprises Ipsec AH with HMAC-MD5 (An apparatus and computer program are able to be a method. Mittra's design has authentication means (column 8, lines 3-10). In authentication, it is very common to use digital signature schemes and hashes. Mittra as to what form of authentication to perform provides no limitation).

24. With regards to claims 35, 56, 82, 94, 117 and 140, Mittra discloses a method wherein the keyed hash function comprises Ipsec AH with HMAC-SHA1 (An apparatus and computer program are able to be a method. Mittra's design has authentication means (column 8, lines 3-10). In authentication, it is very common to use digital signature schemes and hashes. Mittra as to what form of authentication to perform provides no limitation).

25. With regards to claims 39, 86, 98, 121 and 144, Mittra teaches a method further comprising: establishing a security agreement with the designated device using the access information (An apparatus and computer program are able to be a method. Mittra's design uses secure communication (column 4, lines 5-19). Security agreements must be set during secure communication).

26. With regards to claims 41 and 123, Mittra teaches a method further comprising: obtaining the access information for the host device (A computer program is a method. Mittra's design performs authenticating between devices and the GSC (column 4, lines 5-19) (column 8, lines 3-10). During the authentication process the obtaining of the access information as claimed must be performed).

27. With regards to claims 42, 43, 100, 101, 102, 124 and 125, Mittra teaches a method wherein obtaining the access information for the host device comprises: receiving the access information from an access information server prior to receiving the access control message from the host device (An apparatus and computer program are methods. Mittra's design has a GSC that maintains information about the access and authentication information regarding all the devices within the network (column 7, line 64 – column 8, line 2). No limitation was set regarding when data would be obtained by the GSC).

28. With regards to claims 44, 45, 57, 103, 104, 105, 118, 119, 126, 127, 128, 133, 134, 141 and 142, Mittra teaches a method wherein determining whether the host device is authorized to access the shared tree comprises: maintaining an access information database; searching the access information database for the access information for the host device; failing to find the access information for the host device in the access information database; and determining that the host device is not authorized to access the shared tree (An apparatus is a method. Authentication is performed by Mittra's design (column 8, liens 3-10). In addition, all the steps claimed are normal during authentication. Furthermore, the GSC in Mittra's design handles all the group information as claimed (column 7, line 54 – column 8, line 2)).

29. With regards to claims 49, 51, 110, 111, 120, 132, 135, 136 and 143, Mittra teaches a method wherein determining whether the host device is authorized to access the shared tree comprises: determining that the authentication key has expired based upon the expiration date for the authentication key; and determining that the host device is not authorized to access the shared tree; authenticating the host device using the access information and a predetermined authentication scheme; and determining whether the host device is authorized to access the shared tree based upon authenticating the host device using the access information and the predetermined authentication scheme (An apparatus is able to be a method. The claimed steps are known steps during authentication that must be performed. Mittra's design performs

authentication (column 8, lines 3-10). In addition, Mittra's design further allows for the network to be of a tree form (column 4, lines 20-25)).

30. With regards to claims 52 and 112, Mittra teaches a method wherein authenticating the host device using the access information and the predetermined authentication scheme comprises: receiving authentication information from the host device; and authenticating the host device based upon the access information and the authentication information received from the host device (An apparatus is able to be a method. Mittra's design performs authentication (column 8, lines 3-10). In addition, the steps claimed, must occur for the authentication process to function properly).

31. With regards to claim 59, Mittra teaches a method wherein determining whether the host device is authorized to access the shared tree based upon authenticating the host device using the access information and the predetermined authentication scheme comprises: determining that authentication succeeded; and determining that the host device is authorized to access the shared tree (Mittra's design performs authentication (column 8, lines 3-10). In addition, the steps claimed, must occur for the authentication process to function properly).

32. With regards to claim 60, Mittra teaches a method further comprising: establishing a security association with the host device using the access information upon determining that the host device is authorized to access the shared tree (Mittra's

design performs authentication (column 8, lines 3-10). In addition, the steps claimed, must occur for the authentication process to function properly).

33. With regards to claims 63, 70 and 149, Mittra teaches an apparatus wherein the access token comprises: a group identifier for identifying a multicast group; a host identifier for identifying the host device; a token identifier for identifying the access token; an authentication key for the host device; an expiration date for the authentication key; a server identifier for identifying a key server; and a public key for a key server (A communication system and a communication message are able to be a method, computer program and an apparatus. Mittra's design performs authentication (column 8, lines 3-10). During authentication, the access information must contain ids of some form to distinguish it; hence a token identifier along with other identifiers must be present. The presence of identifiers is inherent due to the fact that data is being transferred in between multiple devices and for a variety of reasons. The only way to ensure that such processes function properly is to possess all the identifiers claimed. Furthermore, Mittra discloses the use of a member id that is equivalent to the claimed token identifier (column 7, lines 52-54). In addition, keys are present in Mittra's design (column 8, lines 3-10). And, for an authentication to function properly, it inherently must possess an expiration method of some form).

Remarks

The amended claims have been carefully reviewed, but are not deemed fully persuasive. While numerous claims are presented, the examiner believes that their traits are present within the Mittra prior art.

The applicant's representatives have three points of contention, which they express within the remarks. The amendments made to the claims, reflect these points of contention and the applicant's representatives are convinced that these points demonstrate that the claimed invention is novel. The examiner disagrees and continues to believe that the Mittra prior art embodies the traits claimed. It is important when reading a prior art, to understand the spirit of the design along with it's literal interpretation. The following are brief explanations as to why the points of contention are disagreed upon based on the Mittra prior art.

First, the applicant's representatives remark that the claimed invention possesses a key server, separate from the host. The examiner however would like to point out that such means are also present within the Mittra prior art. Within column 4, lines 53-56, Mittra discloses that if desired, the design can be implemented with key distribution centers. Such devices are separate from the host. Additionally, since the key distribution centers provide a service to clients (distribute keys), it is a form of a server.

Second, the applicant's representatives remark that the claimed invention possesses unique authentication information within the access information. In a network design with authentication processes and multiple hosts, such a feature is

inherent. This is because to each host, the number of clients available and eligible is different. Hence, the authentication information for each must be different.

Finally, the applicant's representatives remark that the claimed invention features access information with expiration date information for authentication keys. Mittra's disclosure teaches that certificates expire and new ones are created and sent with messages (column 11, lines 39-42, Mittra). It was stated before that it is inherent that keys have expiration dates. If authentication data (such as certificates and keys) for devices that join and disconnect from hosts (such as Mittra's) do not have expiration dates, then the authentication data is clearly vulnerable. Since there exists expiration dates for certificates it should be clear that keys have expiration dates as well. Plus it is inherent that since the certificate expiration is noticed and new certificates are sent based on the expiration, that the claimed access information comprising expiration date information is also present within Mittra's design.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Azizul Choudhury whose telephone number is (571) 272-3909. The examiner can normally be reached on M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jack Harvey can be reached on (571) 272-3896. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AC

V. Martin Wallace
Supervisory Patent Examiner